TANG Daogui
FANG Yiping
ZIO Enrico
Laboratoire Génie Industriel, CentraleSupélec
Gif-sur-Yvette, France
Contact : daogui.tang@ecp.fr

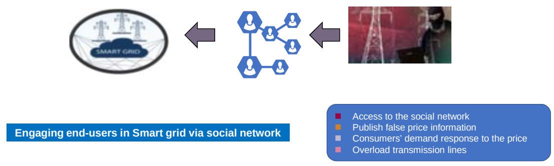
Analysis of the resilience of Smart Grids to Social Network Based Attacks

Background

The integration of social network has attracted much attention to:

- save energy
- reduce peak power consumption
- renewable energy exchange

Social network integration gives chance to malicious attackers to attack the power grid utility service



Proposed models

The multi-level influence propagation model:

- Influence flows from a number of actors to their followers
- An actor can receive influence from his predecessors and pass it through his successors
- Each actor has:
  - an influence level $g \in \{0,1,2,3\}$, representing the extent to which an actor is influenced
    - $g=0$ means the actor is not influenced
    - $g=3$ means the actor is completely influenced
  - an influence weight $w \in \{0,1,2,3\}$, representing the extent to which he is willing to affect his successors
    - The probability distribution of w is given by:

$$y = f(g, B, pt)$$

- *B* represents the benefit from rescheduling consumption
- *pt* represents the personality traits of the actors
  - Influence weights sybergy rules: min, median, max

Customers' response: consumption rescheduling:

- The load at a time slot can be moved to other time slot at some cost
- The goal is to maximize the benefit of consumption rescheduling in the rescheduling horizon

$$\max \sum_{t=t_o}^{t_e} \sum_{t_m=t_o}^{t_e} (\lambda_t^o - c_{tt_m} - \lambda_{t_m}) \cdot \Delta d_{tt_m}$$

Response of the operator: minimize load shedding:

$$\min \sum_{i\in D} s_i$$

$$s.t. \quad -f_{ij}^{\max} \le f_{ij} \le f_{ij}^{\max}$$

$$\sum_{(i,j)\in\delta^+} f_{ij} - \sum_{(j,i)\in\delta^-} f_{ji} = \begin{cases} p_i & i \in P \\ s_i - d_i & i \in D \\ 0 & otherwise \end{cases}$$

$$p_i^{min} \le p_i \le p_i^{max}$$

$$f_{ij} = (\theta_i - \theta_j) \cdot x_{ij}^{-1}$$

$$0 \le s_i \le d_i^r$$

Impact indexes；

- The residual ampacity of transmission lines (*RATL*)

$$RATL_{ij} = 1 - f_{ij} / a_{ij}$$

  - where f_i and a_{ij} are the power flow and ampacity of line (i, j)
- The expected energy not supplied *(EENS)*

$$eens_i = s_i / d_i$$

$$EENS = \sum_{i=1}^{n} eens_i$$

  - where s_i and d_i are load shedding and responsive load at node *i*.

Références

- [1] Pan, T., et al., Threat From Being Social: Vulnerability Analysis of Social Network Coupled Smart Grid. IEEE Access, 2017. 5: p. 16774-16783.
- [2] Huang, Q., et al., Social Networking Reduces Peak Power Consumption in Smart Grid. IEEE Transactions on Smart Grid, 2015. 6(3): p. 1403-1413.
- [3] Mishra, S.L.X.P., et al., Price Modification Attack and Protection Scheme in Smart Grid. IEEE Transactions on Smart Grid, 2017. 8(4): p. 1864-1875.
- [4] Schneider, K., et al., Social network analysis via multi-state reliability and conditional influence models. Reliability Engineering & System Safety, 2013. 109: p. 99-109.

Case study

A modified IEEE 13 node test feeder and a notional social network are adopted as a case study, as is shown in Figure 1:

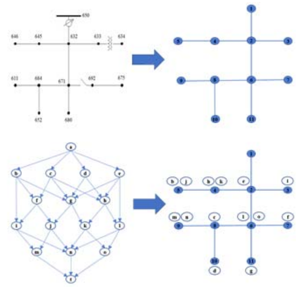


Fig. 1 Modified IEEE 13 node test feeder and the integration of social network.

The historical nodal load data of a day from PJM is shown in Figure 2.

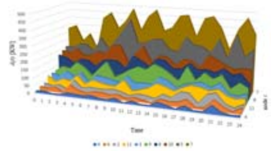


Fig. 2 Nodal load from history data.

The consumption rescheduling result is shown in Figure 3.

Fig. 3 Consumption rescheduling.

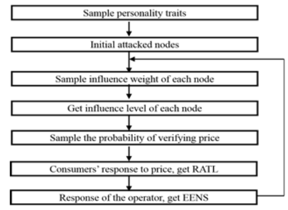


Fig. 4 Flowchart of MCS process.

The Monte Carlo Simulation (MCS) is illustrated in Figure 4.

Result and conclusion

Result analysis of attacking:

- given false information sources: actor *b*, *c*, *d* and *e,* denoted as scenario 1.
- actor *b*, *c*, …, *t*, respectively; denoted as scenario 2, 3, …, 16, respectively.

The distribution of the indexes with MCS is as follows.

Result of scenario 1:

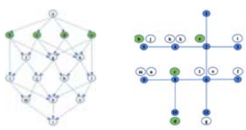


Fig. 5 Attacked actors in scenario 1.

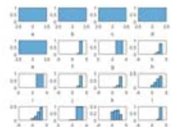


Fig. 6 Influence level distribution.

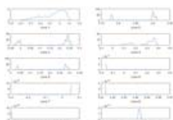


Fig. 7 *RATL* distribution.

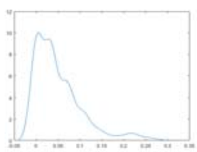


Fig. 8 *EENS* distribution.

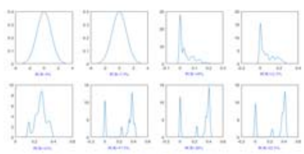


Fig. 9 *EENS* distribution under different PCR.

Comparative result of different scenarios

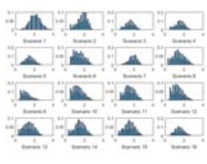


Fig. 10 Mean influence level distribution.

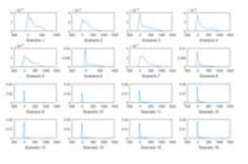


Fig. 11 Average load increase distribution.

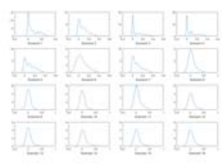


Fig. 12 *EENS* distribution.

- Conclusion
  - There is a limit to the impact of the system by increasing PCR.
  - The impact of SNFPA on SN and SG is highly relative, especially for those scenarios which will cause high influence.
  - In general, attacking more actors in social networks will have a higher influence, but that's not absolute.
  - Even though the social network is as a relatively low overall influence level, directly attacking the actors with high power demand in power grid will have large influence on the SG.

Research Group Safety & Risks
Laboratoire Génie Industriel